

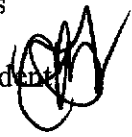
This e-mail has been approved by Dr. Frieda K. Lacey, deputy superintendent of schools.

Office of Special Education and Student Services
MONTGOMERY COUNTY PUBLIC SCHOOLS
Rockville, Maryland

February 16, 2007

MEMORANDUM

To: All Principals
All Special Education Service Providers

From: Carey M. Wright, Associate Superintendent 

Subject: Suggested Guidelines for Protecting Personally Identifiable
Student Information in Electronic Media Formats

Through the implementation of Encore and other data systems, the Office of Special Education and Student Services is expanding the use of electronic media to more efficiently manage the paperwork associated with special education and student services. As a result, all staff must become more aware of best practices that are designed to protect the privacy rights of students when electronic media is used. The privacy and data protection guidelines attached are from Dr. Carol Ann Baglin, assistant state superintendent, Division of Special Education/Early Intervention Services, Maryland State Department of Education. Staff should review and follow these guidelines to ensure the protection of privacy for all students. If you have any questions, please contact Mr. Paul Bruening, Encore project manager, Department of Special Education Operations, by calling 301-279-3166.

CMW:bjh

Attachment

Copy to:
Executive Staff
Mr. Bruening
Ms. Mason
Ms. Strange Moscoso
Dr. Newman

Approved: 
Frieda K. Lacey, Deputy Superintendent of Schools

**Suggested Guidelines For Protecting Personally Identifiable Student Information
In Electronic Media Format
Provided by the Maryland State Department of Education
January 2007**

The confidentiality of personally identifiable student information must be preserved whether the information is in paper or electronic format. Electronic media allows school system personnel the ability to transport voluminous amounts of personally identifiable student information to use and work with at a wide range of locations and allows teachers, related service providers, and administrators to electronically store personally identifiable student information. Electronic media can be an electronic computing device such as a laptop or desktop computer, PDA, or other devices that accept diskettes, compact disks, DVDs, tapes, memory sticks, or any other type of removable storage device.

Remember, regardless of the format, personally identifiable student information remains subject to and is covered by federal confidentiality laws (FERPA and IDEA) and Maryland state law. School system personnel who use and work with electronic media containing personally identifiable student information must take reasonable steps to protect electronic data from unauthorized access, alteration, loss, destruction, and/or disclosure. Failure to take care of this personally identifiable student information in electronic media format places students and their families at risk of identity theft and misuse of personal information. It also puts local school systems at risk for violation of applicable federal and state confidentiality laws.

The Maryland State Department of Education (MSDE) suggests that school systems take steps to educate their personnel about methods to best protect personally identifiable student information when it is transported off-site by electronic media. MSDE offers the following suggested guidelines concerning maintaining confidentiality of personally identifiable student information.

1. Students' name or Social Security Number should not be used in the subject line, message body, or attachments to e-mail.
2. Students' personally identifiable information should not be stored on any home computer or electronic media that is not appropriately secured, i.e., password protected or encrypted.
3. Students' personally identifiable information should be limited only to individuals who require access to fulfill that person's work obligations.
4. Current anti-virus and *[spyware]** software should be installed on off-site computers where personally identifiable student information will be stored.
5. Personally identifiable student information should be securely removed from electronic media before re-using the electronic media or disposing of it.
6. Make an inventory of the personally identifiable student information that is transported by electronic media.
7. Limit the amount of personally identifiable student information stored on mobile electronic media to the minimum necessary needed to do your job.
8. Secure portable electronic media devices containing personally identifiable student information as if they contained your personal information. Do not leave devices in unattended vehicles, unlocked offices, or unsupervised in common areas.

**[added by Montgomery County Public Schools]*